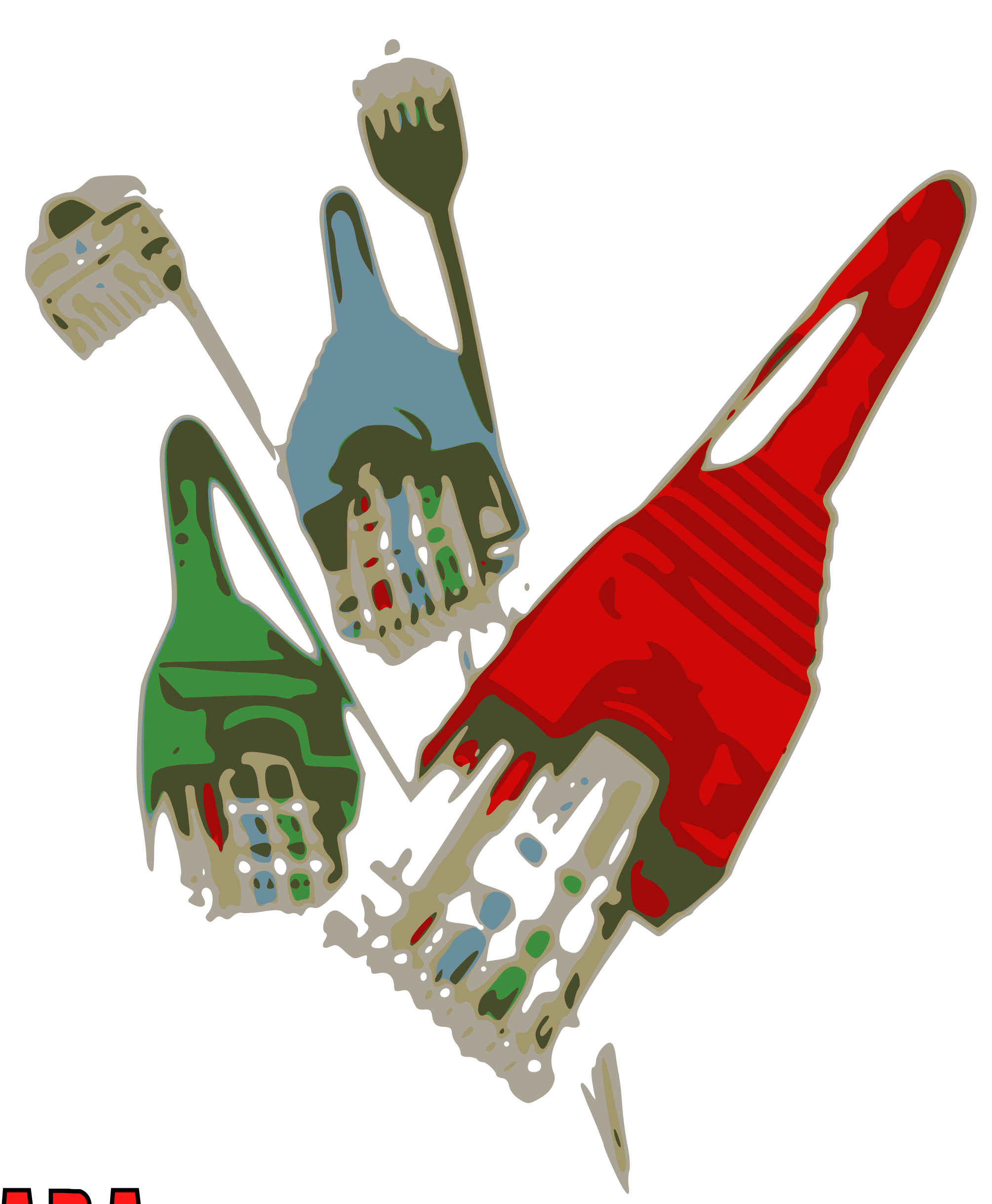
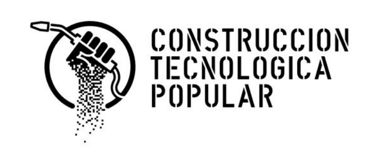
SEGURIDAD



PARA:

MILITANTES Y COMUNICADORES





VER 1.0

Introducción

Esta pretende ser una pequeña guia de herramientas y recomendaciones que son solo un primer paso para reducir la vulnerabilidad en la seguridad digital y privacidad de militantes y comunicadorxs en la Argentina en la coyuntura actual.
Debemos tener siempre presente, como principio básico, que estas herramientas no son 100% inviolables y no ofrece garantías de que nadie pueda espiarnos, pero si que, quien lo quiera hacer, tenga las cosas un poco más difíciles. Aunque la internet se ha vuelto la herramienta mas completa de vigilancia a la sociedad civil, sigue siendo para el Estado, y sus aparatos represivos, los métodos tradicionales igual de efectivos, como es el caso de la infiltración de agentes en las organizaciones. En el mismo sentido es que creemos que nuestros medios y organizaciones tienen que tener como pilar los metodos tradicionales de seguridad. Las nuevas tecnologías son un eslabón más que tenemos que conciderar.
Debemos tener en cuenta, a diferencia de los viejos métodos de espionaje, que el paradigma de los mismos ha cambiado, la maquinaria de espionaje no descansa y su funcionamiento eficiente es, por definición, no restrictivo sino silencioso. No reactivo sino retroactivo. No individual ni dirigido sino masivo.
Encontraremos aquí programas de software gratuito como así software libre (o código abierto).
Debido a la vorágine de la evolución tecnológica que corren en estos tiempos, debemos advertir que este manual y las herramientas que presentamos, son algo provisorio. Sirve, sí, pero solo por ahora, no sabemos mañana, ni mucho menos dentro de unos años.
También, como pilar fundante de este material, queremos expresar nuestra firme convicción de que la seguridad y la privacidad de nuestros datos y comunicaciones son una construcción colectiva. Es por esto mismo que debemos participar de forma consciente cada unx de lxs actores en la comunicación.
Este manual fue creado, principalmente, a partir de dos grandes fuentes:
Security in a Box y manual Cryptoperiodismo
A quienes agradecemos profundamente sus esfuerzos por el material brindado.

Principios Básicos

Sin importar cuales sean tus más amplios objetivos, el mantener tu computadora libre de problemas es un primer paso indispensable en la senda de una mejor seguridad. Por ello, antes de empezar a preocuparte demasiado - por ejemplo, acerca de contraseñas sólidas - comunicación privada y encriptación de archivos, necesitas garantizar que tu computadora no sea vulnerable a los piratas informáticos (hackers) o no esté plagada de software malicioso (malware), tales como virus y software espía (spyware). De lo contrario, es imposible garantizar la efectividad de cualquier otra precaución de seguridad que pudieras tomar. Después de todo, no tiene sentido cerrar la puerta si el policia ya se encuentra adentro de nuestra casa, y tampoco es bueno empezar a subir por las escaleras si dejas la puerta completamente abierta.
Vamos a recomendar algunas herramientas para Windows, ya que es el sistema mas vulnerable a estos ataques, aunque usuarios que tengan GNU/Lunux y Apple OS no se encuentran exentos.

Virus

Existen muchas maneras distintas de clasificar los virus, y cada una de estas viene acompañada de su propia colección de categorías con nombres pintorescos. Gusanos, macrovirus, troyanos y puertas traseras (backdoors) son algunos de los ejemplos más conocidos. Muchos de estos virus se extienden en Internet, utilizando el correo electrónico, páginas web maliciosas u otros medios para infectar computadoras no protegidas. Otros se propagan a través de medios extraíbles, particularmente a través de pendrives y de discos duros externos que permiten a los usuarios escribir y leer información. Los virus pueden destruir, dañar o infectar la información en tu computadora, incluyendo datos en discos externos. Estos también pueden tomar control de tu computadora y utilizarla para atacar a otras. Afortunadamente existen muchas herramientas antivirus que puedes utilizar para protegerte y proteger a aquellos con los cuales intercambias información digital.
ast antivirus

avast! es un programa antivirus con funciones completas que detecta y elimina software malicioso (malware) y virus de tu computadora. Aunque avast! es gratuito para uso no commercial en el hogar o en una computadora personal, tu copia gratuita debe ser registrada después de la instalación; de lo contrario, expirará en 30 días. El registro también garantiza que recibas automáticamente las últimas versiones de avast! y las actualizaciones de la base de datos de virus a medida que se encuentren disponibles.
Podes descargarlo del siguiente link:
http://www.avast.com/es-ww/index

Software Espía (Spyware)

El software espía (spyware) es una clase de software malicioso (malware) que puede rastrear el trabajo que haces, tanto en tu computadora como en la Internet, y enviar dicha información a alguien que no debe tener acceso a ella. Estos programas pueden registrar, entre otras cosas, las palabras que digitas en tu teclado, los movimientos de tu ratón, las páginas que visitas y los programas que ejecutas. Como resultado de ello, pueden socavar la seguridad de tu computadora y revelar información confidencial sobre ti, tus actividades y tus contactos. Las computadoras se infectan con software espía (spyware) en prácticamente la misma forma en la que contraen virus. Debido a que las páginas web maliciosas son la mayor fuente de infecciones de software espía (spyware), debes prestar mayor atención a los sitios web que visitas y asegurarte que las opciones de tu navegador sean seguras.

Software contra Software espía (spyware)

Puedes utilizar herramientas contra software espía (spyware) para proteger tu computadora de este tipo de amenazas. El Spybot es uno de esos programas, y hace un buen trabajo identificando y eliminando ciertos tipos de software malicioso (malware) que los programas antivirus simplemente ignoran. Sin embargo, de la misma manera que con un programa antivirus, es extremadamente importante que actualices las definiciones de software malicioso (malware) del Spybot y que ejecutes escaneos regulares.
Podes descargarlo de:
http://www.safer-networking.org/

Cómo generar contraseñas seguras

Las claves de acceso a los dispositivos y a los servicios Web son, frecuentemente, una fuente de problemas. Implican una gestión difícil y es muy fácil terminar simplificándolas, o de los contrario, corriendo riesgos serios para poder recordarlas. Son puertas de acceso que, una vez abiertas por terceros, no hay nada que hacer excepto, en el mejor de los casos, esperar a volver a tomar el control pero habiendo perdido información y, sobre todo, privacidad.
Un buen diseño de las claves que usas a diario reduce sensiblemente las probabilidades de que un dispositivo o un servicio Web sea vulnerado, aunque es claro: nada es 100 % seguro.
Quienes intentan violar contraseñas ajenas frecuentemente lo hacen mediante tres métodos bien diferenciados, de complejidad variable y aplicados a distintos contextos: ataques de diccionario, ingeniería social y acceso físico a un dispositivo.
Un ataque de diccionario es un método de cracking basado en la "fuerza bruta". Es poco inteligente pero no por eso poco efectivo. Consiste en averiguar contraseñas probando múltiples combinaciones de caracteres miles de veces hasta dar con la correcta. Un robot genera las combinaciones e intenta acceder con cada una de ellas. Hasta que no encuentra aquella que busca y le permite acceder, no se detiene.
La ingeniería social es otra de las tres grandes compuertas para vulnerar contraseñas. Es una práctica para obtener información sobre la víctima y, a partir de ella, dar con la clave que se busca o tener los datos que permiten recuperarla. El método actualmente está en pleno auge ya que la cantidad de información personal que se hace pública a diario en las redes sociales está creciendo de un modo inconmensurable. En las redes sociales circula la materia prima con la que se produce buena parte del espionaje actual.

El acceso físico a un dispositivo es un riesgo también creciente. Cada vez usamos más dispositivos conectados a la Red. Todxs. Y todo parece indicar que esa tendencia continuará en ascenso durante los próximos años. La mayoría guarda contraseñas en sus dispositivos. Los navegadores de las computadoras y las aplicaciones de los dispositivos móviles son verdaderos paraísos para el espionaje. El acceso físico muchas veces es la llave maestra que abre todas, o casi todas, las demás puertas.
En esta parte ofrecemos algunas sugerencias para crear y gestionar claves de un modo seguro, que reduzcan al mínimo las probabilidades de ser conocidas y usadas por terceros.

Paso a paso

Para empezar, lo esencial es descartar la estrategia de la memoria fácil: fechas de nacimiento, números de documentos de identidad o pasaporte, números de teléfono, apodos, nombres de parientes y mascotas, direcciones de lugares que puedan ser asociadas con vos, edad, ciudades, barrios, códigos postales, etc.

Toda esa información es demasiado predecible. Descartarla a la hora de crear contraseñas equivale a dejar fuera de juego la posibilidad de que alguien con tiempo, cercano o un desconocido con acceso a tu información, se tome el trabajo de intentar "adivinar" sus passwords y, con un poco de suerte, acertar.
De hecho, existen servicios Web que solicitan ese tipo de información. En ese caso, lo más recomendable es no usarlos. Si no tiene más opción que hacerlo, mienta: no publique su dirección, teléfono o código postal, por ejemplo.
Su segunda misión es sacarse de la cabeza que es algo seguro usar la misma clave de acceso para todo. De hecho esa estrategia implica todo lo contrario: es lo más inseguro que podes hacer.

Un algoritmo para crear passwords seguras puede ser el siguiente:

1. Vos, como todos nosotros, recordás una frase o título de un libro, el estribillo de una canción, una cita, una película, etc. Lo primero que debes hacer es seleccionar aquella frase que recordás con precisión pero que no lo representa ante su entorno social. Es decir, aquella que sabes que es muy improbable que pueda serte asociada.
2. Una vez identificada esa frase debes seleccionar solamente una letra de cada palabra que la compone. Pongamos por ejemplo, la primera letra. Aunque lo más recomendable sería que use la segunda, o la tercera, etc., o una combinación. Por ejemplo, si la frase que eligió es "Nunca sería socio de un club que me aceptara como miembro", el nemónico tomando la primera letra de cada palabra sería "nssducqmacm". Ya dio un primer paso, está más lejos de la inseguridad. Pero vaya más allá.
3. Añada una variable más, una letra en mayúsculas. La tercera por ejemplo: "nsSducqmacm".
4. Tome en cuenta el servicio Web para el que está creando esa clave, por ejemplo "mail.google.com". Elija la marca o alguna palabra con la que Usted lo asocie mentalmente. Si es la marca, en este caso, sería "google". Si es una palabra, podría ser "correo". Ahora complete su contraseña: una esta variable a la clave generada en los tres puntos anteriores con un signo, por ejemplo, "!". El resultado es "google!nsSducqmacm" o bien "correo!nsSducqmacm".
5. Un último agregado para terminar de crear su clave: añada un número y otro símbolo. Por ejemplo ";12". Su contraseña es ahora: "google!nsSducqmacm;12" o bien "correo!nsSducqmacm;12".

Ahora bien, esta clave le permitirá acceder a su cuenta de correo en Google. Modifíquela para cada
servicio extra que use. Por ejemplo, para su clave de Twitter, podría ser: "Twitter!nsSducqmacm;12".

Siguiendo estos cinco pasos es posible crear una contraseña fuerte a nivel de seguridad y relativamente simple de recordar.
El método reduce el margen de inseguridad pero no es infalible.
Si al servicio al que estas accediendo con esta clave no la almacena de un modo seguro, su clave es
tan vulnerable como si fuera "1234567890"

Pidgin + OTR

Pidgin es un cliente de mensajeria instantanea, multi plataforma, en el cual puedes agregar tus diferentes cuentas de chat al mismo tiempo. Esto significa que puedes chatear con tus contactos de MSN, Google talk, yahoo, facebook, etc. al mismo tiempo. Funciona de forma similar bajo windows o bajo linux



Existe un complemento que se llama OTR - Off-the-Record (Fuera de Registro) esta desarrollado específicamente para Pidgin. Este ofrece las siguientes características de privacidad y seguridad:
Utiliza cifrado de principio a fin (end-to-end): desde tu equipo al de la persona con la que estás hablando.
Autenticación: Se te garantiza que tu correspondiente es quién tu crees que es.

Rechazo: Despúes de finalizada la sesión de conversación (chat), los mensajes no pueden ser identificados como procedentes de ti o de tu correspondiente.

Cifrado: Nadie mas puede acceder ni leer tus mensajes instantáneos.

Perfecta Seguridad Adicional: Si terceros obtienen tus claves privadas, ninguna de tus conversaciones anteriores estará en peligro.

Básicamente, hay 3 pasos involucrados en la configuración adecuada del OTR para posibilitar efectivamente sesiones de MI privadas y seguras y estos son explicados a continuación:

Primer Paso: Este involucra la generación de una llave privada única asociada con tu cuenta, y que muestra su huella digital.

El siguiente paso involucra el aseguramiento de la sesión de MI y la autenticación de tus amigos.

Segundo Paso: Este involucra la solicitud de una parte de una sesión de mensajería privada y segura con la otra parte actualmente en línea.

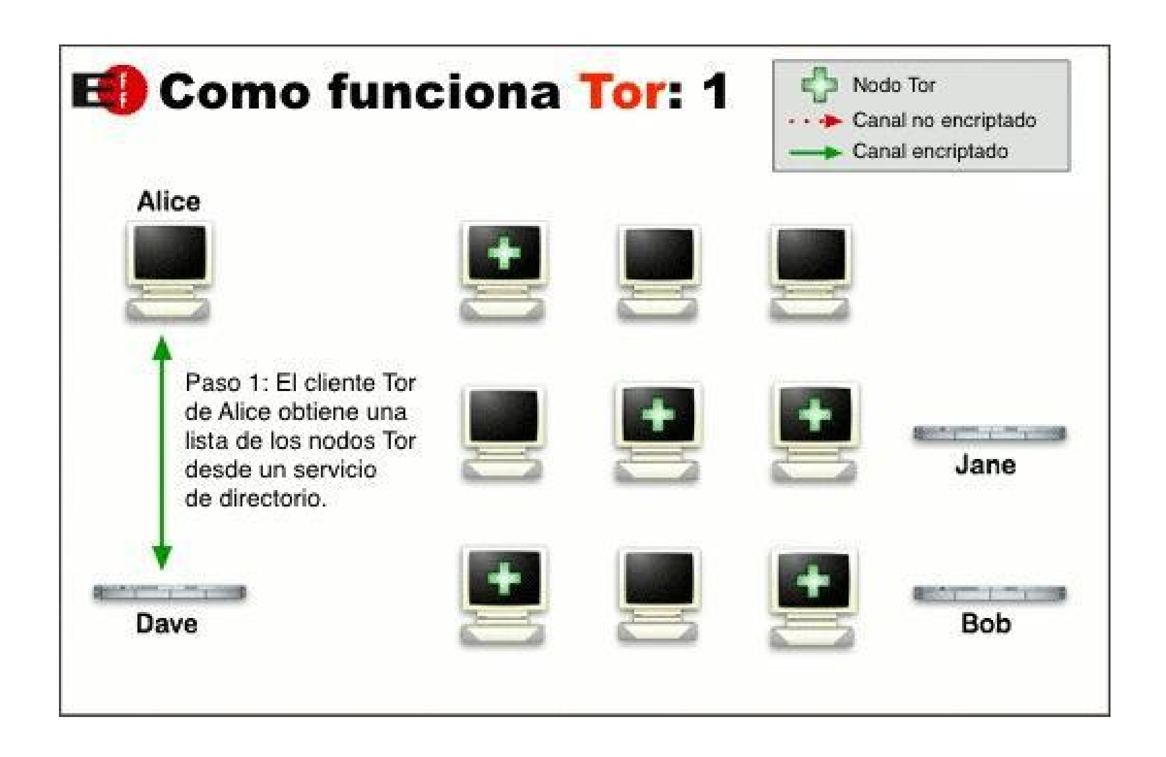
El Tercer Paso implica la autenticación o verificación de la identidad de tu amigo en Pidgin. (Nota: Esto significa determinar que tu amigo es exactamente la persona quien dice ser por medio

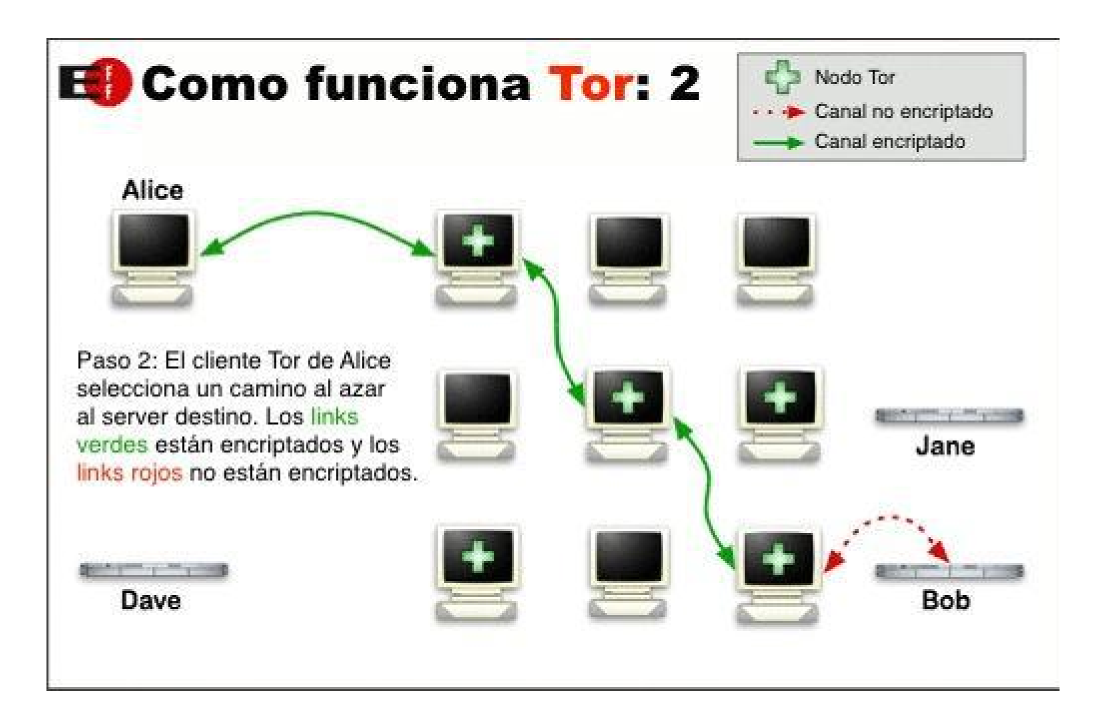
Mantenerse anónimo al navegar por Internet

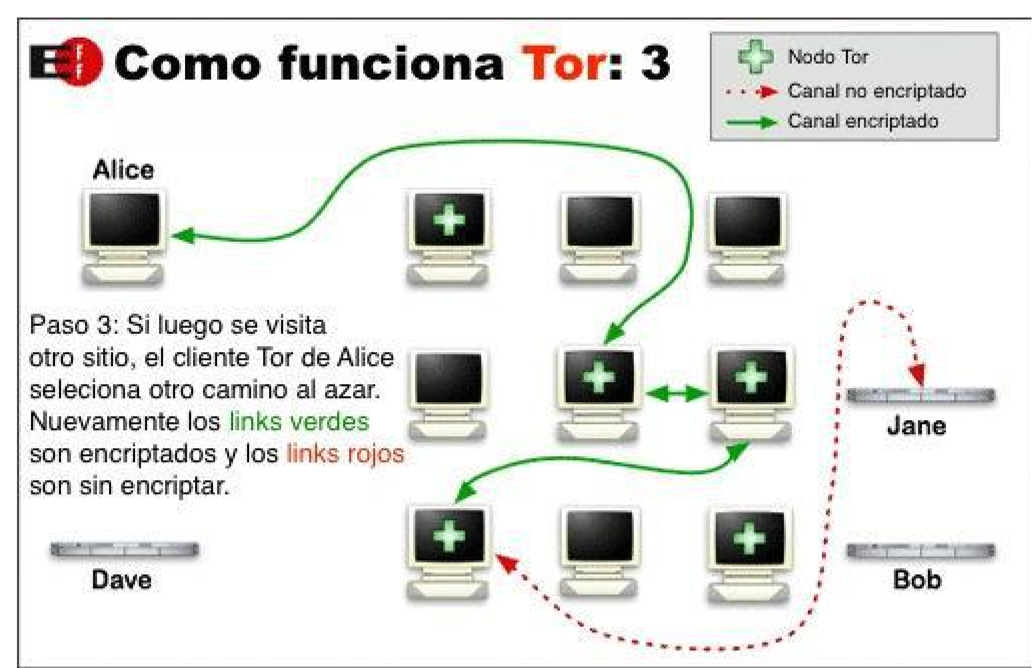
El proyecto Tor intenta permitir navegar anónimamente por Internet. Esto lo logra utilizando una red de voluntarios que ejecutan servidores para cambiar la ruta por la que un usuario navega por la Red,permitiendo ocultar la información que da cuenta sobre desde dónde se origina la visita. Tor no solamente altera la ruta sino que también encripta múltiples veces los datos, lo que hace extremadamente difícil conocer su origen y su contenido. De todos todos, hay que tener muy claro esto antes de avanzar: el valor agregado de Tor no es proteger el contenido sino anonimizar los datos de quien está navegando.
Originalmente Tor fue creado por el Laboratorio de Investigación Naval de Estados Unidos para proteger las comunicaciones de gobierno. Actualmente es usado por una comunidad cada vez mayor de hackers, y muy especialmente por activistas, periodistas profesionales de distintas áreas que trabajan con información sensible.

Cómo funciona Tor

Tor crea una suerte de 'túneles' por donde van pasando los datos. En vez de seguir una línea recta entre el usuario y el sitio al que se quiere conectar, Tor crea un camino alternativo. Cada vez que pasa por un túnel, la información se vuelve a encriptar y es enviada hacia el siguiente túnel, hasta alcanzar el punto de salida, donde se conecta al sitio de destino.
En todo el trayecto, cada uno de los túneles no conoce el camino completo. Sólo conoce el túnel anterior de donde vino y hacia dónde tiene que enviarlo a continuación, nada más.
Para crear este camino, Tor utiliza un software especial que le permite conocer cuáles son los servidores disponibles y así seleccionar la ruta autilizar. Este software permite también que cada diez minutos se pueda volver a cambiar la ruta y de esa forma no poder relacionar las acciones que se venían haciendo con las futuras acciones que realice el usuario.







Un punto a tener en cuenta es que Tor opera desde la máquina del usuario hasta el último servidor antes de llegar a destino. El camino que va desde el último servidor al destino no está protegido y los datos relacionados a ese tráfico son visibles.

Tor no resuelve todos los problemas de anonimidad. Por ejemplo la información que presenta el navegador al conectarse al servicio destino puede ser una fuente para obtener datos del usuario.

Correo electrónico



Existen algunos pasos importantes que puedes dar para incrementar la seguridad de tu comunicación por correo electrónico.
El primero es cambiarse a una cuenta de correo electrónico mas segura.
“Pocos proveedores de correo con interfaz web ofrecen el acceso Capa de Conexión Segura (SSL) a tu correo electrónico. Por ejemplo, Yahoo y Hotmail, proporcionan una conexión segura cuando inicias sesión, para proteger tu contraseña, pero tus mensajes en sí se envían y reciben de manera insegura. Además, Yahoo, Hotmail y otros proveedores de correo con interfaz web incluyen la dirección IP de la computadora que estas utilizando en todos los mensajes que envías.
Las cuentas de Gmail, por otro lado, utilizan una conexión segura desde el inicio de sesión y todo el tiempo hasta que hayas cerrado la sesión. Puedes comprobarlo todo el tiempo viendo y observando el URL que inicia con 'https', en la que la 's' denota una conexión segura. A diferencia de Yahoo y Hotmail, el Gmail no revela tu dirección IP a tus destinatarios de correo. Sin embargo no es recomendable que confíes completamente en Google para la confidencialidad de tus comunicaciones electrónicas sensibles. Google escanea y guarda el contenido de los mensajes de sus usuarios para una gran variedad de propósitos y, en el pasado, ha sido condesciente con demandas de los gobiernos que restringen la libertad digital.
Si es posible, debes crearte una nueva cuenta de correo electrónico en Riseup visitando https://mail.riseup.net. Riseup ofrece correo electrónico gratuito a los activistas alrededor del mundo y presta mucha atención a la protección de la información almacenada en sus servidores. Ellos por mucho tiempo han sido una fuente confiable para aquellos con necesidad de soluciones seguras de correo electrónico. Y, a diferencia de Google, tiene políticas muy estrictas relativas a la privacidad de sus usuarios.” (securityinabox - https://securityinabox.org/es/chapter_7_1)

Otro paso para obtener un alto grado de privacidad en las comunicaciones mediante correo electrónico es utilizar un cliente de correo electrónico, como el Thunderbird, que es el que recomendamos usar, junto con el plugin Enigmail , que es una de las formas más simple de utilizar PGP para encriptar los correos tanto en Linux, Mac o Windows.

Pretty Good Privacy (PGP) es un software para encriptar y desencriptar información. PGP utiliza un método de encriptación denominado de clave pública o asimétrico. Consiste en la utilización de dos claves que funcionan en conjunto. Una, la privada, es tenida a resguardo por el propietario y jamás divulgada. La otra, la pública, puede ser distribuida libremente por cualquier medio.

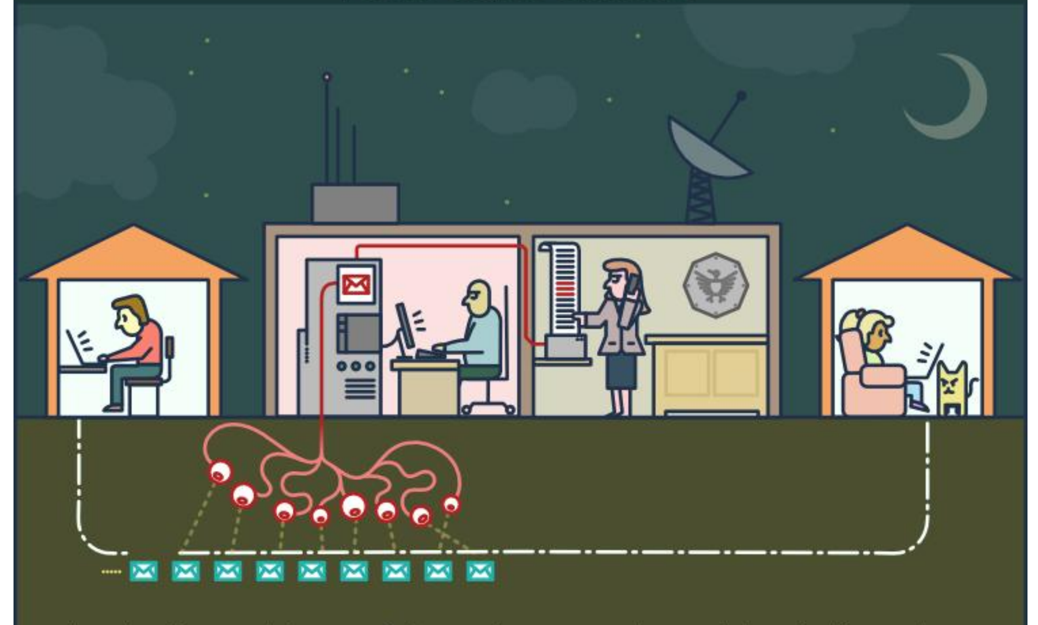
La única forma de desencriptar ese mensaje es utilizando la clave privada, cuyo único poseedor es el destinatario. Ninguna persona que posea la clave pública del destinatario podrá desencriptar el mensaje. De esta manera se puede enviar un mensaje encriptado por una red pública como Internet sin temor a que su contenido pueda ser visto.

Dejamos el link de una guía bastante buena y fácil de seguir para poder configurar nuestras computadoras para enviar correos electrónicos utilizando PGP.

DEFENSA DEL CORREO

La vigilancia indiscriminada viola nuestros derechos y compromete la libertad de expresión.

Pero no estamos indefensos.



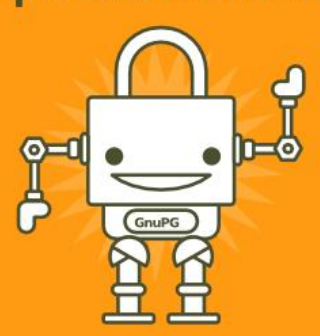
La contraseña que protege tu correo electrónico es tan solo una delgada capa de seguridad que no puede protegerte contra el ariete de los sistemas sofisticados de vigilancia.

Cada mensaje pasa por muchos sistemas informáticos en ruta hacia su destino. Las agencias de vigilancia lo aprovechan para leer millones y millones de correos electrónicos.

Incluso si no tienes nada que ocultar, cuando envías un correo normal, las personas con las que te comunicas quedan también al descubierto.

¡Recupera tu privacidad con GnuPG!

Solo necesitas un sencillo programa llamado **GnuPG**. Cifra tu correo de modo que solo puede leerlo la persona adecuada.



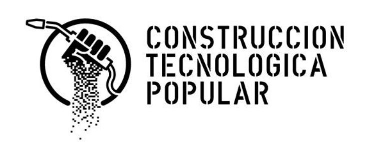
GnuPG funciona en casi cualquier computadora o smartphone. Su licencia es libre y es gratuito. Cada usuario tiene una **clave pública** y una **clave privada** únicas, que son cadenas aleatorias de números.



TU CLAVE PÚBLICA

Tu clave pública no es como una llave física, porque se comparte. Está en una guía en línea, desde donde otras personas pueden descargarla. Usarán tu clave pública, junto con GnuPG, para cifrar los correos que te envíen.







RED NACIONAL DE MEDIOS ALTERNATIVOS



TU CLAVE PRIVADA

Tu clave privada es más parecida a una llave física, ya que la guardas solo para ti (en tu computadora). Usas GnuPG y tu clave privada para descifrar los correos cifrados que otras personas te envían.





Si un correo cifrado con GnuPG cae en las manos equivocadas, no tendrá ningún sentido. Sin la clave privada del destinatario, es casi imposible leerlo.

Para el verdadero destinatario, se abre como un correo normal. ¡Fácil!

El remitente y el destinatario están ahora más seguros. Incluso aunque este correo no contenga información confidencial, al estar cifrado fastidia a los sistemas de vigilancia. **¡Toma ya, vigilancia!**



GnuPG es **software con licencia libre**; es completamente transparente y cualquiera puede copiarlo o crear su propia versión. Esto hace que sea más seguro contra la vigilancia que el software patentado (como Windows o Word). Aprende más en **FSF.org**.

Para protegernos contra la vigilancia, debemos aprender a utilizar GnuPG y comenzar a **compartir nuestras claves públicas** cuando compartimos direcciones de correo electrónico.

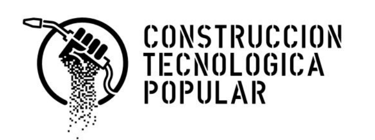
Miles de personas usan ya GnuPG: activistas, periodistas, quienes denuncian ilegalidades y gente corriente. Con cada usuario nos fortalecemos y demostramos a las agencias de vigilancia que estamos dispuestos a defendernos.

Aprende a defender tu correo. Aprende GnuPG en 30 minutos en

EmailSelfDefense.FSF.org









Usar motores de búsqueda alternativos

Una de las actividades más recurrentes que se hace habitualmente en Internet es realizar búsquedas en los motores de búsquedas, como por ejemplo Google, Bing y Yahoo, si queremos sortear en parte el espionaje que se nos puede realizar deberíamos esquivar estos buscadores ya que todos recopilan nuestra información personal, dejan guardadas nuestras búsquedas e información sensible a nuestras conexiones con la cual nos pueden rastrear.
Las agencias de seguridad no son las únicas que recaban, clasifican y ordenan los datos personales para hacer el perfil de los individuos. De hecho, esa es una de las grandes especialidades de los gigantes de la web: Yahoo, Google y Amazon.

Podemos recomendar dos buscadores:

DuckDuckGo pone la privacidad en el centro de su política, prometiendo no recabar ni compartir información sobre sus usuarios.
https://duckduckgo.com/



Startpage es un navegador que posee clústeres de servidores en los Países Bajos y Estados Unidos y proporciona la búsqueda anónima a través de un servidor proxy gratuito.
https://startpage.com/esp/

Cambiar servicios de elaboración de documentos

Otras herramientas muy utilizadas en nuestra cotidaneidad en internet, son los documentos colaborativos y si pretendemos salir de los sistemas de vigilancia no debemos usar herramientas como Google Docs, Microsoft Office Web Apps y Zoho Office Suite. Aunque parezcan los únicos viables, en realidad hay varios más disponibles que son un poco más seguros. RiseUP es un servidor autogestionado especialmente para movimientos sociales, donde los datos de tus documentos estarán a salvo. Etherpad es un editor web colaborativo, que utiliza colores para señalar a los diferentes usuarios y se basa en la privacidad. Ethercalc es el mismo servicio que el anterior, pero con hojas de cálculo.

Recomendaciones:

pad.riseup.net es un servidor autogestionado que da servicio a multitud de movimientos sociales de todo el mundo.
https://pad.riseup.net/

Etherpad es un editor web basado en la colaboración en tiempo real, lo que permite a los autores editar simultáneamente un documento de texto y ver a todos los participantes de las ediciones en tiempo real, con la posibilidad de mostrar el texto de cada autor de diferente color.

Ethercalc es un servidor de hojas de cálculo multiusuario.
https://www.ethercalc.org/

Dudle sistema de encuesta en línea gratis con una versión privacidad mejorada opcional.

Utilizar los teléfonos móviles de la manera más segura posible

Los teléfonos móviles son una parte integral de nuestras comunicaciones diarias.
Todos los teléfonos móviles tiene la capacidad para servicios de mensajería de voz y de texto simple. Su bpequeño tamaño, relativamente bajo costo y muchos usos hacen de estos dispositivos invaluables para todos que cada día los utilizamos más para propósitos de comunicación y organización.
La forma en la que la red móvil opera, y su infraestructura, son esencialmente distintos a aquellos como funciona la Internet. Esto crea retos adicionales a la seguridad, y riesgos para la privacidad de los usuarios y la integridad de su información y comunicaciones.
Con la aparición de los SmartPhone que se pueden contar con GPS, tienen capacidad multimedia (registro de foto, video y audio y a veces su transmisión), procesamiento de datos y acceso a la Internet dificulta aun más nuestra meta por la seguridad y privacidad en las comunicaciones, ya que ahora este dispositivo aparte de ser un teléfono es una computadora y hay que considerar la mayoría de los consejos anteriores.
Debemos tener en cuenta que las redes de telefonía móvil son redes privadas administradas por entidades comerciales, las cuales pueden estar bajo el control monopólico del gobierno. La entidad comercial (o gubernamental), tiene prácticamente acceso ilimitado a la información y a las comunicaciones de sus clientes, así como la capacidad para interceptar llamadas, mensajes de texto, y vigilar la ubicación de cada aparato (y por tanto de sus usuarios). Los proveedores telefónicos en la mayoría de países están legalmente obligados a mantener registros de todas las comunicaciones. Las comunicaciones de voz y texto también pueden ser intervenidas por terceros en las proximidades al teléfono móvil, utilizando equipo de bajo costo.
Con el fin de enviar o recibir llamadas o comunicaciones de cualquier tipo desde y hacia tu teléfono, la antenas de señal más cercanas son alertadas, sobre tu presencia, por tu teléfono móvil. Como parte de su operación normal, cada teléfono móvil automáticamente y de manera regular informa al proveedor del servicio telefónico donde está en determinado momento. Es más, muchos teléfonos hoy en día tienen funciones de GPS, y esta información precisa sobre la ubicación podría ser incorporada en otros tipos de datos tales como fotos, el servicio de mensajes cortos (SMS) y en solicitudes de Internet que son enviadas desde el teléfono.

Buenas prácticas en seguridad telefónica

Como en el caso de otros dispositivos, la primera línea de defensa para la seguridad de la información en tu teléfono móvil es la protección física de tu teléfono móvil, y de su tarjeta SIM de ser tomadas o manipuladas.
Siempre utiliza tus códigos de bloqueo de tu teléfono o los Números de Identificación Personal (PINs) y mantenlos en secreto (desconocidos para otros). Siempre cámbialos para que no sean lo que coloca el fabricante.
Asegúrate de ser consciente de la información que está almacenada en tu tarjeta SIM, en tarjetas adicionales y en la memoria de tu teléfono. No almacenes información sensible en el teléfono. Si necesitas almacenar dicha información, considera colocarla en tarjetas de memoria externas que puedan ser fácilmente desechadas en caso necesario - no coloques tales detalles en la memoria interna del teléfono.
Protege tu tarjeta SIM y tu tarjeta adicional de memoria (si tu teléfono tiene una), pues estas podrían contener información sensible tales como detalles de contacto y mensajes SMS. Por ejemplo, asegúrate de no dejarlos en la tienda de reparaciones cuando tu teléfono esta siendo arreglado.

Si planeas obsequiar, vender o reutilizar tu teléfono asegúrate que toda la información sea eliminada.
Haz regularmente copias de seguridad en tu computadora de la información que se encuentra en tu teléfono. Almacena la copia de seguridad de manera segura. Esto te permitirá restaurar los datos si pierdes tu teléfono. Tener una copia de seguridad también te ayudará a recordar que información podrías estar en peligro (cuando tu teléfono se haya perdido o haya sido robado), de modo que puedas tomar las acciones pertinentes.
El número de serie de 15 dígitos o número IMEI te ayuda a identificar tu teléfono y puede ser accedido tecleando *#06# en la mayoría de teléfonos, viendo detrás de la batería en tu teléfono o revisando las especificaciones del mismo. Toma nota de este número y mantenlo alejado de tu teléfono, pues este número podría ayudar a rastrear en caso sea robado y a probar la propiedad del mismo rápidamente.

Sobre escuchas secretas

Tu teléfono puede ser preparado para registrar y transmitir cualquier sonido dentro del rango de alcance de su micrófono sin tu conocimiento. Algunos teléfonos pueden ser encendidos de manera remota y puestos en acción de esta manera, aún cuando parezcan estar apagados.

- Nunca permitas que las personas de quienes desconfías tengan acceso físico a tu teléfono; esta es una manera común de instalar software espía en tu teléfono.
- Si estas conduciendo reuniones privadas e importantes, apaga tu teléfono y desconecta la batería. O no lleves el teléfono contigo si no puedes dejarlo donde pueda estar completamente a salvo.
- Asegúrate de que cualquier persona con la que te comuniques también emplee las acciones descritas aquí.
- Además, no olvides que utilizar un teléfono en público, o en lugares en los que no confías, te hacen vulnerable a las técnicas tradicionales de escucha secreta, o que te roben el teléfono.

Sobre intercepción de llamadas

Generalmente, el cifrado de las comunicaciones por voz (y por mensajes de texto) que viajan a través de la red de telefonía móvil es relativamente débil. Existen técnicas de bajo costo que pueden utilizar terceros para interceptar tus comunicaciones escritas, o para escuchar tus llamadas, si están en la proximidad de tu teléfono y pueden recibir transmisiones desde el mismo. Y por su puesto, los proveedores de telefonía móvil tienen acceso a todas tus comunicaciones de voz y texto. Actualmente es costoso y/o de alguna manera técnicamente difícil cifrar las llamadas telefónicas de modo que incluso el proveedor de telefonía móvil no pueda escucharlas secretamente - sin embargo, se espera que estas herramientas pronto se vuelvan económicas. Para utilizar el cifrado primero tendrías que instalar una aplicación o programa de cifrado en tu teléfono, así como en el dispositivo de la persona con la cuál planeas comunicarte. Entonces utilizarías esta aplicación para enviar y recibir llamadas y/o mensajes cifrados. El software de cifrado actualmente sólo puede ser admitido en unos cuantos modelos llamados teléfonos 'inteligentes'.

Comunicaciones textuales SMS / Mensajes de texto

No debes confiar en los servicios de mensaje de textos para transmitir información sensible de manera segura. Los mensajes intercambiados son en texto simple lo que los hace inapropiados para transacciones confidenciales.
El envío de mensajes SMS puede ser interceptado por el operador de servicio o por terceros con equipo de bajo costo. Dichos mensajes llevan los números telefónicos del emisor y del receptor así como el contenido del mensaje. Lo que es más, los mensajes SMS pueden ser fácilmente alterados o falsificados por terceros.

Privacidad con los celulares?

Debemos recordar, como dijimos antes, que el celular para que funcione normalmente debe estar todo el tiempo comunicado con las antenas de telefonía mas cerca para poder establecer la comunicación. Este es su principio de funcionamiento y no se lo puede modificar. Por lo que, si el móvil o la tarjeta SIM, están asignados a una persona, esta es fácilmente rastreable y localizable por las companias telefónicas, entidades gubernamentales o terceros, con muy pocos recursos económicos.
Los celulares son dispositivos de transmisión, y mientras la batería este conectada, existe una pequeña posibilidad de que de alguna manera alguien pueda encenderlo sin que lo sepas, por lo que debes extraer la batería en caso de una reunión que prende ser confidencial.
Dicen que hay programas que pueden ser instalados en tu teléfono para secretamente encenderse a distancia y llamar a un número telefónico sin tu conocimiento. Entonces, al momento que empiezas tu reunión, este empezaría a actuar como un dispositivo de grabación y transmisión. Esto es muy fácil de hacer desde el punto de vista tecnológico. Pero nada de ello puede suceder si la batería esta desconectada, de modo que estarás a salvo en este improbable caso.
Solo tenes que saber cuáles son los beneficios y los riesgos del uso de estos dispositivos. Se cuidadoso. Si conoces los riesgos, puedes dar los pasos necesarios para evitarlos.

Palabras finales

Nuestra intención no ha sido, ni es, impartir paranoia, sino generar conciencia y conocimiento que es nuestra mayor herramienta.
Hemos recorrido algunos consejos y herramientas para que, ahora que sabemos un poquito más, podamos tener esas consideraciones al momento de entablar una comunicación sensible por medio de estos canales.



Por otra parte el uso las herramientas antes mencionadas, que ya es una gran paso, pensá en establecer un sistema de código entre vos y tus compañeros. Los códigos podrían hacer tu comunicación más segura y podrían proporcionar una forma adicional de confirmar la identidad de las personas con las que te estas comunicando. Los sistemas de código necesitan ser seguros y cambiar frecuentemente.

Recordando lo que dijimos al principio, sostenemos que la seguridad y la privacidad es una construcción colectiva por lo que debemos fomentar en nuestros espacios la disciplina de usar estas prácticas y herramientas

Como Contactarnos?
ctp@ctpcordoba.com.ar
www.ctpcordoba.com.ar